



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/182,279	10/29/1998	DON COPPERSMITH	Y0998-313	1845
30743	7590	01/18/2005	EXAMINER	
WHITHAM, CURTIS & CHRISTOFFERSON, P.C. 11491 SUNSET HILLS ROAD SUITE 340 RESTON, VA 20190			NGUYEN, CUONG H	
		ART UNIT	PAPER NUMBER	
		3661		

DATE MAILED: 01/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/182,279	COPPERSMITH ET AL.
	Examiner	Art Unit
	CUONG H. NGUYEN	3661

- The MAILING DATE of this communication appears on the cover sheet with the correspondence address -

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 01 December 2004.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-13 and 15-23 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-13, 15-23 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 10/29/98 is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a))

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ .

5) Notice of Informal Patent Application (PTO-152)

6) Other: ____ .

DETAILED ACTION

1. This Office Action is the answer to: the RCE, the preliminary amendment (37 C.F.R. 1.114) received on 8/12/2003, the interview conducted on 12/01/2004, and the proposed specification amendment received on 12/01/04 at 12:34 pm. Claims 1-13, 15-23 are pending.

Priority

2. This application claims priority of a provisional application having a priority date of 4/14/1998.

Interview

3. On 12/01/2004, the examiner initiated an interview with the applicants' representative (Mr. C. Lamont Whitham). The reviewer/(director assigned business-method specialist) advises that claim 1 is a "broad" claim. The examiner talked to the applicant's representative about further distinguishing the claimed subject matter but he did not want to amend the claim, only arguing about a distinguishing specification.

For "broad" claim 1, the inventors claim "a system" but a required structure (i.e., a memory) MUST be done via another means - to verify a product is authentic - (that is EXTERNAL to that claimed system, furthermore, "for verifying that a product is authentic" is merely an intent of use, e.g., that electronic tag can be used for many different purposes, not necessary for authentication). Please note that with regard to the concept of verification without revealing authentication information, applicants admit this

is prior art on page 7, lines 25-32 (see zero-knowledge protocols); and the applicants delete a further limitation of "reading encrypted information" to broader claimed scope in this RCE.

In claim 1, there is no explicitly recited verification step, it just appears as "reading said authentication information ... to verify"; as a result, the details of the authentication may not to have weight here and the recited structure would read on conventional tag/reader systems. Even if the authentication was given weight, as mentioned above, applicants already admit that zero-knowledge protocols are known, see the specification, page 7.

4. These following pertinent references have the same subject matter with the pending application; specifically the references of Goldman, and Berson were told to Mr. Michael Witham on 6/2003 (Mr. C. Lamont Whitham was not available). Mr. Michael Witham gave these pertinent references to IBM Corp. for further reviews to result in a submitted RCE; however, the amended limitations are not supported by the specification (i.e., "based solely on the information contained in said memory"); Mr. Michael Witham further argues that "IBM was the first to use this available technology (zero-knowledge protocols) for product authentication"; the examiner respectfully submits that this is not an inventive idea (about "IBM was the first to use...").

5. On 1/04/05 and 1/06/05 the examiner called the applicant's representative for a formal amendment to overcome 35 USC 112, 1st issue as proposed in the 12/01/2004 facsimile transmittal (i.e., "based solely on the information contained in said memory"); however, the applicants' representative was not available. This Office Action will also indicate that issue.

- **Goldman**, (US Pat. 4,785,290 - 11/15/1988), Non-counterfeit able document system, wherein a system comprises a cryptographically encoded tag (T) having encoded information on the tag for verification. This encoded information are compared with signals from a database; hence, that tag is used as identification means in shelf life and sales channels.

- **Bellare** et al., (US Pat. 5,673,318 - 9/30/1997), Method and apparatus for data authentication in a data communication environment; this invention teaches a receiving component generates a second tag which can then be compared with the transmitted tag to determine message authentication (determining an authentication tag) - applicants argue that the product is the object for the authentication, not the tag (see the facsimile transmittal 12/01/2004), the examiner respectfully submits that it is old and well-known for authentication based solely on a product.

- **Berson**, (US Pat. 5,768,384 - 6/16/1998), System for identifying authenticating and tracking manufactured

articles; wherein a tag encrypted information is affixed to the manufactured article; a data center coupled to the manufacturing meters and located at a site remote from the manufacturing meters; means for producing information that identifies the manufactured articles; and a plurality of means located where the authenticity of the manufactured articles are checked by comparing the encrypted information on the article with the information produced that identifies the article.

- **Carlson's** patent was cited because the applicants argue that "private/public keys, or encryption technique or decryption technique" were not disclosed in previous cited references .

6. The examiner is unpersuasive with claimed concept of protecting goods against counterfeiting using smart tags that the applicants presented. The examiner submits that the use of smart cards, (or electronic tags - a derivative of smart cards) is obvious for one with skill in the art, it contains many different information because it has a memory chip, including routing information (see previously cited references of Finast, or Bank Marketing Magazine, or Retail Automation, or Laurie Petersen; see also the article title "Metrorail to take a high-tech trip with smart card" by the Washington Post, published on 7/05/1998; it provides some background for a technology of using smart card). This article said that: "Smart cards -- which have been around

for years in Europe", and (for the reader) "to known how many riders it has, but also who they are, where they get on the subway, where they go, and even what they have for lunch", and "Embedded in the card is a small computer chip that stores data. When the card is passed over the gate's reader, its antenna sends a signal to the gate to open. Computer chip: Holds approximately 30 times the data that can be stored on a magnetic-stripe card", and "Card reader: Rider passes card in front of the machine's reader to begin a transaction and again at the end of the transaction to register any changes", and "Non-contact smart card reader: Card is passed within three inches of reader. Riders can pass their entire wallet or purse over the disk. Display window shows how much is on the card", these information suggest an obvious use of smart card/smart tags/electronic tags in reading the information contained inside those cards/tags; from there, a purpose of protecting goods against counterfeiting is analogously achievable.

7. The examiner respectfully submits that Fuji clearly identifies GemPlus as a company that in a business of manufacturing, at least, and GemPlus' product obviously having analogous limitations as applicants claimed about GemPlus's electronic tags using in retailed business (Fuji's article obviously suggest about smart/electronic tags using in retailed stores (see FUJI-KEIZAI USA, INC. pg.1, e.g.

electronic tags, and GPR400, a smart card reader in PC Card format to instantly encrypt and decrypt reading data).

Applicants argue that: "the article does not teach or suggest attaching a smart card to a product or goods such the authenticity of the good can be readily verified", the examiner submits that the concept of using smart card for authenticity/(getting secure/correct information), the suggestion of attaching a electronic tag/(smart card) to a product for a purpose is just an intend of use. The smart card/electronic tag, itself, contains secured information to trace/authenticate, among other things, original sources.

8. On 12/02/2004, SPE Wynn Coggins decided to make a rejection after reviewed of the cited evidences, and comments of the business-method specialist. The examiner regrets for any delay this may cause.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 1-23 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. These claims contain subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with

which it is most nearly connected, to make and/or use the invention, that is "based solely on the information contained in said memory" (please note that zero-knowledge protocols also use private/public key pairs - see page 7 of the specification).

10. Taking into account above 35 USC 112, 1st paragraph rejections (assuming there is no support for above 35 USC 112, 1st issue); as best interpretation, the examiner analyzes claims as followings based on what were supported by the specification.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office Action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. **Claims 1-3, 5-6, 8-10, 15-16, 18** are rejected under 35 U.S.C. § 103(a) as being unpatentable over Werb et al. (US Pat. 6,150,921), in view of an article of

FUJI-KEIZAI USA, INC.

A. Referring to claim 1: Werb et al. suggest a system for verifying an authenticity of a product, comprising:

- a tag is attached to a product, it can store authentication information; and a reader for reading said authentication information from said tag.

In page 5, para.2 of the argument received on 2/27/2002, the applicants admits that "The Fuji-Keizai

reference describes the use of a smart card with encrypted data. However, it can be seen that the article deals only with data storage and retrieval concept". The examiner submits that this reference in combination of Werb et al. clearly suggests the use of an electronic tag. Artisan would appreciate WHY these smart tags were manufactured, and WHERE these smart tags would be placed. However, this is an intent of use, this reference doesn't need to disclose that information.

The above limitations are obviously included in GEMPLUS product (see FUJI-KEIZAI USA, INC. pg.1, e.g. electronic tags, and GPR400, a smart card reader in PC Card format to instantly encrypt and decrypt reading data); (see also an example of Chew (US. Pat. 5,901,303) suggests a similar application (e.g. a tag having a memory) with a microprocessor embedded in a smart card).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use a readily available information/system on the market from GEMPLUS with Werb et al.'s suggestion for verifying a product because they suggest using an electronic tag with memory, and a scanning component at POS to display related product information.

B. Re. to claim 5: It is quite obvious to one with skills in the art to further (with the given rationale and references for rejection in claim 1) including a reader/scanner (for

authenticating a product) in front of a consumer prior to purchase of the product (see *In re Larson*, 144 USPQ 347 (CCPA 1965) for about integration available components in the market for POS verification/authentication tasks in claim).

C. Re. to claim 6: It is quite obvious to one with skills in the art to further (with the given rationale and references for rejection in claim 1) including a reader/scanner for reading an electronic tag without physically contacting said tag (see FUJI-KEIZAI USA, INC. pg.1, e.g. RF/ID products from GEMPLUS do not need physically contacting a tag for reading information e.g., using a small laser beam).

D. Re. to claim 8: It is very well-known to one with skills in the art to further (with the given rationale and references for rejection in claim 1) imply that authenticating product information is directed to a product 's manufacturer (e.g. a company names "Sony" making a Sony product).

E. Re. to claim 9: It is very well-known to one with skills in the art to further (with the given rationale and references for rejection in claim 1) indicate that authentication information is for a specific product (e.g. utilizing a product serial number).

F. Re. to claim 10: It is very well-known to one with skills in the art to further (with the given rationale and references for rejection in claim 1) including a label having authentication information printed thereon to be

verified against the authentication information read by a reader (e.g. a label imprinted with a product serial number).

G. Re. to claim 18: This claim has a similar limitation as claim 10 although it is written for a method claim; hence, the same rationales and references are incorporated.

H. Re. to claim 15: It is obvious to one with skills in the art (with the given rationale and references for rejection in claim 1) to have authentication information including information for authenticating an electronic tag (e.g. a manufacturer, its location .etc., e.g. Sony in Japan).

In summary, the same analysis, references, and reasoning set forth in the rejection of claim 1 are applied to these claims also because they are directed to a system that comprises similar means with very obvious limitations.

12. Claim 2 is directed to a system for verifying an authenticity of a product, wherein a tag is a smart card (see FUJI-KEIZAI USA, INC. pg.1, e.g. electronic tags, and GPR400, a smart card reader in PC Card format to instantly encrypt and decrypt reading data); (see also an example of Chew (US. Pat. 5,901,303) wherein they suggest a similar application (e.g. a tag having a memory) with a microprocessor embedded in a smart card).

13. Claim 3 is directed to a system for verifying an authenticity of a product, wherein a tag is attached/embedded into a product/(a product packaging) (see e.g. see also an example of Storch et al. (US Pat.

5,367,148) Figs. 2-3, the rationales for rejection for claim 1 are incorporated).

14. Claim 4 is rejected under 35 U.S.C. § 103 as being unpatentable over Werb et al. (US Pat. 6,150,921), in view of an article of FUJI-KEIZAI USA, INC., and further in view of Mob (US Pat. 5,740,250).

Werb et al., suggest a system for verifying an authenticity of a product. They do not disclose that information is encrypted using a private key, and is decrypted using a public key.

However, Mob suggests information is encrypted using a private key, and is decrypted using a public key (see **Mob**, claims 21, and 26; the rationales for rejection for claim 1 are incorporated herein).

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of GEMPLUS (FUJI-KEZAI USA), and Werb et al. with the suggestions of Mob for verifying the authenticity of a product in a conventional way (using private-public keys to decrypt information), because this would enhance extra security for a trusted verification/authentication.

15. Claims 7, and 17 are rejected under 35 U.S.C. § 103 as being unpatentable over Werb et al. (US Pat. 6,150,921), in view of an article of FUJI-KEIZAI USA, INC., and in view of Guillou et al. (US Pat. 5,140,634).

Claims 7 is directed to a system for verifying an authenticity of a product, wherein a zero-knowledge protocol is used (see Guillou et al., the abstract, the rationales

for rejection for claim 1 are incorporated herein - please note that utilizing "zero-knowledge protocol" is Applicant Admitted Prior Art in the submitted specification).

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of Werb et al. and GEMPLUS with the suggestions of Guillou et al. for verifying the authenticity of a product using "zero-knowledge protocol", because this is readily available in the market at that time, and the verifying system would be done in a conventional way.

16. Re. to claim 17: This claim has a similar limitation as claim 7 although it is a method claim; hence, the same rationale and references are incorporated for an obvious rejection.

17. Claim 11 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Werb et al. (US Pat. 6,150,921), in view of an article of FUJI-KEIZAI USA, INC., and in view of Storch et al. (US Pat. 5,367,148).

A system for verifying the authenticity comprises a product serial number.

The rationales for rejection for claim 1 are incorporated herein.

Werb et al., teach about using a serial number of a tag. FUJI-KEIZAI INC.'s article do not expressly disclose above limitation.

However, Storch et al. also show that this limitation is very well-known (see at least Storch et al., Fig. 3).

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of Werb et al., and GEMPLUS with the suggestions of Storch et al. 's disclosure for verifying the authenticity of a product serial number, because this information is very well-known for relating to specific information of manufacturing a product, and the verifying system would be sufficient with a product's serial number.

18. Claim 12 is rejected under 35 U.S.C. § 103 as being unpatentable over Werb et al., and an article of FUJI-KEIZAI USA, INC.

As best interpretation, it is directed to a system for verifying the authenticity comprises a graphical image/indicia (of the product) (this limitation is very well-known on the market, e.g. an apple for an "Apple computer" .etc., the rationales and references for rejection for claim 1 are incorporated herein).

19. Claims 13, 20 are rejected under 35 U.S.C. § 103 as being unpatentable over Werb et al. (US Pat. 6,150,921), in view of an article of FUJI-KEIZAI USA, INC., in view of DiCesare et al. (US Pat. 5,971,435).

A. Re. to claim 13: As best interpretation, it is directed to a system for verifying the authenticity comprises an ownership history (of the product).

The rationales and references for rejection of claim 1 are incorporated herein.

Werb et al., and FUJI-KEIZAI USA, INC.'s article do not expressly disclose of using an ownership history of the product for authentication.

However, DiCesare et al. suggest that limitation (see DiCesare et al., 4:40-56, and claim 13).

It would have been obvious to one of ordinary skill in the art at the time of invention to implement the system of Werb et al., and GEMPLUS with above suggestion of DiCesare et al. for verifying the authenticity of a product, because a product's past ownership history is considered by the artisan as critical information for authentication.

B. Re. to claim 20: This claim has a similar limitation as claim 13 although it is a method claim; hence, the same rationales and references set forth are incorporated for an obvious rejection.

20. **Claim 19 is rejected under 35 U.S.C. § 103 as being unpatentable over Werb et al. (US Pat. 6,150,921), in view of an article of FUJI-KEIZAI USA, INC., and further in view of Matyas et al. (US Pat. 5,164,988).**

The rationales and references for rejection for claim 1 are incorporated herein.

It has an extra limitation of verifying the authenticity, wherein (authentication) information is erased after being read.

Werb et al., and FUJI-KEIZAI USA, INC.'s article do not expressly disclose above limitation.

However, Matyas et al. show that this limitation is very well-known (see Matyas et al., 19:25-26, and 20:2-4).

It would have been obvious to one of ordinary skill in the art at the time of invention to implement Werb et al.,

and Gemplus's system with a suggestion of Matyas et al. for verifying the authenticity of a product, because these claimed technique is already available at that time, and the verifying task would be known as "done" with that product, and saving memory space.

21. **Claim 21** is rejected under 35 U.S.C. § 103 as being unpatentable over Werb et al. (US Pat. 6,150,921), in view of an article of **FUJI-KEIZAI USA, INC.**, in view of Matyas et al. (US Pat. 5,164,988), and further in view of **DiCesare et al.** (US Pat. 5,971,435).

Comparing to preceding claims, **Claim 21** has an extra limitation of "detecting counterfeit products in a market", the examiner respectfully submits that this limitation is merely an intent of use of the system in pending claim 1 (the purpose of the claim is merely FOR authentication, and "verifying routing information" is covered with "checking ownership history", this feature is already analyzed from pending claim 13 based on DiCesare et al.'s reference.

Therefore, it only has a feature that is different from above claims 1-20: verifying a routing information of a product (other similar meanings that are claimed for above step are obvious for one with skills in the art, e.g. ownership histories). Upon reviewing, above limitation is obviously suggest with GemPlus smart tags because the tags contain a memory; therefore, routing information obviously must be written in a said memory "chip".

It would have been obvious to one of ordinary skill in the art at the time of invention to implement Werb et al., and GEMPLUS's system with a suggestion of Matyas et al., and DiCesare et al., in Fuji-Keizai 's electronic tags for verifying the authenticity/information of a product, because these information/technologies are readily available at that time, and the verifying task would be obviously included for a product.

22. Claims 22-23 are rejected under 35 U.S.C.S 103(a) as being unpatentable over Werb et al. (US Pat. 6,150,921), in view of an article of FUJI-KEIZAI USA, INC, and further in view of Carlson et al. (US Pat. 4,758,714).

The rationales and references for rejection for claim 21 are incorporated herein.

Werb et al., and FUJI-KEIZAI USA, do not disclose about encrypting authentication information with a private key, and decrypting said encrypted authentication information at POS.

However, as indicated in prior Office Action, Carlson et al. al disclose that public/private keys, encryption/decryption techniques at point-of-sales have been used. They also disclose that a verification step is done and routing information was used for satisfactorily verification.

(Carson et al.'s patent discloses that: "This invention anticipates the use of checks as they currently exist using the Fed MICA system. However, a modified check may be used in the future which is a standard check save for the

addition of an "NCR" (no carbon required) slip on the back entitled D-8 and a mag-stripe adhered to the front labeled D-17/D-18 shown in FIG. 11. The NCR page would include the amount of the check, D-16 and the serial number of the check D-15 as well as the company's logo and other regulated information. It may or may not include the duplication of the payer's signature and countersignature, D-11 and D-13. However, it would naturally reproduce the Payee's name, D-12 and the date, D-14. D-11 and D-13 could possibly be obscured by a vision blocking ink screen such as seen on common personal checks with NCR pages. However, a preferred method to handle personal checks, Gov't checks, Travelers checks or any negotiable instrument using the Fed's MICA system would be to utilize the optional "dot matrix" or comparable type printer together with the optional alphanumeric keypad at 2-10 (15-10 and 14-10) and the onboard CPU's and verification circuitry to automatically contact the issuer's bank computer, electronically transfer the required funds directly to the payee's bank account ("electronic funds transfer" also known as "EFT") and then cancel the check or instrument in the device all at the point-of-sale. This would be accomplished in much the same way as EFT is used with bank credit cards today. Those skilled in the art will readily recognize that this method is preferred should applicable laws allow. The scenario of the EFT/POS-CANCELLATION will be as follows: Mr. XYZ is out of town and wants to make a purchase at a stranger's establishment. He

would present his check, already filled out in full as per customary procedures. The retailer would punch in the check amount at 2-10 which would read out at 2-23 for the retailer and the customer to see and then place the check in the device and close the 1-2 lid. The customer would then enter his personal identification number at the PIN keypad. It should be noted here that the machine will only take a PIN entry a certain number of second before the 1-2 lid is closed and will accept a PIN entry only a certain number of second after the 1-2 lid is closed. This is to help prevent a "residual" PI entry from incorrectly hindering a legitimate sale and enhance the security of the device. When the 1-2 lid closes the device's CPU (which may or may not contain the customer's PIN entry at this time) will trigger the function of the MICA read head assembly to "read" the data on the check. If a mag-stripe is located on the check, it will also read that information. The CPU will then compare the PIN entered by the customer to that interpolated from the MICA information. This interpolation process may utilize the onboard algorithm modules in the module drawer or may depend upon outboard interpolation. Outboard interpolation would allow each bank to solely hold their own encryption /decryption methods and algorithm thus maintaining a higher state of security. Returning to the scenario; if the onboard CPU cannot interpret the PIN match up, then it would automatically call up the MICA network and using the routing and transit numbers on the face of the

check would locate the very bank this particular check issued from. The MICA information sent from the onboard CPU would enter the bank's computer via suitable circuitry whereupon the bank's computer would use the encryption/decryption methods and/or algorithms known only to it to make the PIN comparison. For example, the bank's computer may use a combination of routing and transit numbers, account numbers and even individual check numbers in conjunction with their own security algorithm (known only to this bank's computer and perhaps key personnel) to arrive at a PIN which would either match or not match with that entered by the customer at the point-of-sale. At an appropriate time, the bank's computer would be told the amount of the check and its individual number as supplied by the POS terminal, examine whether the customer's balance is sufficient to cover the check, receive the payee's bank number and account number, and if all functions are deemed desirable, the payer's bank computer would electronically transfer the funds and debit the payer's account. The payee's routing and transfer and bank numbers and the payee's account number would be transferred to the payer's bank computer only after a satisfactory PIN match had been made. It should be noted that the POS device described herein can be programmed with the retailers (payee's) routing and transit numbers, bank numbers and account numbers quite easily via the 2-10 keypad by qualified personnel. Then, after the EFT had taken place,

the payer's bank computer would wire the appropriate check cancellation information to the POS terminal which would then (A) print it on the back of the check via the dot matrix printer and (B) if the "daily totals" option is onboard, would add the amount of the EFT to the daily total. The 1-2 cover would then pop open and the cancelled check would be presented to the customer as part of his receipt. Thus, the banks are shifting much of their check handling to the point-of-sale".

In Detailed Description Text portion (para. 43), **Carson et al.**'s patent discloses that:

"FIGS. 13 and 16 show an alternative design to that discussed so far in this section. This alternative design more readily accommodates traveler's checks, personal checks, food stamps, etc. and in fact constitutes refinement and improvement over that system shown in FIGS. 5 and 6. A MICA reader device, 14-76, 15-76, and 16-76, such as that in common use by the Federal Reserve Banking System is installed adjacent to the 13-36 (14-36 and 15-36) mag-stripe reader head. This is possible since the three mag-stripe tracks on common credit cards and the MICA line on all checks are in such close proximity as shown by Figure 15. Due to strict Standard's regulations, this phenomenon is likely to remain indefinitely. As has been previously stated, the selection of which "head" to use is automatically made prior to verifier movement by the

system's CPU in association with the switches numbered 15-18, 15-18A and 15-86. The position of the MICA, PIN, or offset number on the 15-78 check is shown at 15-75A and will be read as a part of the routing and transit numbers and account numbers preceding it in the MICA line.".

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use above conventional technique as Carlson's suggestion for authentications in Werb et al., and FUJI-KEIZAI USA because this technique of using private-public key pairs for encryption and decryption is sufficiently secure and is trusted.

Conclusion

23. These following references are related to this invention however, they prove that claimed concept is not original.

- FUJI-KEIZAI USA, INC., "Top 40 high tech companies in Europe: GEMPLUS, FRANCE: Analysis of factors/strategies for company's success, future plans and business opportunities in this industry", published on July 1997.
- Goldman, (US Pat. 4,785,290 - 11/15/1988), Non-counterfeitable document system, wherein a system comprises a cryptographically encoded tag (T) having encoded information on the tag for verification. This encoded information are compared with signals from a database; hence, that tag is used as an identification means in shelf

life and sales channels. This reference concerns with different approach of preventing counterfeiting of manufactured goods.

- Berson, (US Pat. 5,768,384 - 6/16/1998), System for identifying authenticating and tracking manufactured articles; wherein a tag encrypted information is affixed to the manufactured article; a data center coupled to the manufacturing meters and located at a site remote from the manufacturing meters; means for producing information that identifies the manufactured articles; and a plurality of means located where the authenticity of the manufactured articles are checked by comparing the encrypted information on the article with the information produced that identifies the article. This reference concerns with different approach of preventing counterfeiting of manufactured goods.

- GIAMPAPA MARK EDWIN et al., METHOD AND APPARATUS FOR AUTOMATED MEASUREMENT OF PROPERTIES OF PERISHABLE CONSUMER PRODUCTS, Patent Number: WO0045331 (US) - G06K19/07, Publication date: 2000-08-03. This patent is directed to a method and apparatus for reporting dynamic properties of a product using radio frequency identification device technology. With this invention, an electronic tag (100) is equipped with a sensor (101) which determines dynamic properties of a product when the tag (100) is activated. The dynamic properties of the product are then either further

processed into other dynamic properties. In any event either the former or the latter dynamic properties are then transmitted from the tag (100). Such dynamic properties could be the temperature of a product or the expiration date of the product derived from periodic measurements of the temperature of the product.

- ANDERSSON HAKAN (GB), Method and system for controlling meat products, Patent Number: US2003062001, (WO03027718), Publication date: 2003-04-03

IPC Classification: A01K29/00 ;The present invention relates to a method and a system wherein an animal (10) at birth is provided with at least one electronic tag (20), comprising communicating means and an identification code. The code represents a specific location in a network-connected database (60,) being updated wirelessly (50) from the tag (20) to at least one receiver (40) connected to the position determining means and a time determining means and in connection with said network, registering time- and positioning information related to the animal (10).

Additional information about the animal is provided to the database (60). The registered information is utilized for authorizing at least one of slaughtering and distributing actions for the purpose of at least one of meat production, meat product manufacturing and breeding. An electronic tagging of each piece of meat cut up at the time of

slaughter is performed, each additional tag comprising communication means and a code connecting to said database (60) location, registering time- and positioning information related to the meat via said receiver. When refining the meat into packaged products a scanning and removing of the tags from the cut-up pieces of meat is performed and each packaged product is subsequently provided with a replacement tag comprising communication means and a code connecting to at least one database (60) location, registering time- and positioning information related to the meat product via said receiver.

- COUSTERE FREDERIC et al., Product management system based on non-contact electronic tags, storing data in tag memory relating to product attributes which can be read and modified by interrogating stations interfaced with computer during product lifetime; Patent Number: FR2800186; Publication date: 2001-04-27; IPC Classification: G06F17/60. This invention is about the use of electronic tags in product, each product to be monitored carries an electronic tag (10) with at least one memory storing product attribute information. An interrogation station (40) performs reading and writing of information from and into the memory (22). At least one data processing device (64) communicates via an interface (60) with the interrogation station to interpret

data read from the tags and to determine which data should be read from and written into them.

- EBERHARDT MARK E JR, ELECTRONIC TAGS INCORPORATING A CUSTOMER ATTRACTING ANNUNCIATOR FOR USE IN ELECTRONIC PRODUCT INFORMATION DISPLAY SYSTEMS, Patent Number: WO0067240

Publication date: 2000-11-09, IPC Classification: G06F 17/60. This invention is about an electronic tag having a customer attracting annunciator such as a light emitting element or sound element is provided. In one aspect, a tag constructed for sideward direction of lighting is provided. In another aspect, a battery free tag including a customer attracting annunciatate which is energized with power derived from induced signals developed in the tap. In a further aspect, an annunciator of an electronic tag is controlled based upon signals output form an LCD display driver.

- TAKEDA NABUO et al. (JP), METHOD OF AND SYSTEM FOR IDENTIFYING MEDICAL PRODUCTS; Patent Number: WO0033246, Publication date: 2000-06-08; IPC Classification: G06K19/07. This invention is about an electronic tag for identifying a medical product. A miniature passive transponder (15) comprises a power coil (21) for coupling power into the passive transponder, a power regulator (23) for regulating power to all on-board circuits, a memory (25) that contains identifying data for the medical product, a VCO (27)

converting the stored data into a signal compatible for mixing, by a mixing circuit (31), with a signal of an RF oscillator (29), and an amplifier (33) for amplifying the mixed signal prior to transmission via an antenna (35) to an external monitoring system (17). Power generated from a field generator (19) of the monitoring system (17) is coupled into the transponder (15) power coil (21) to enable receipt of the memory data at an RF receiver (37) of the monitoring system (17). The RF receiver (37) connects to a CPU (39) to facilitate demodulation of the received RF signal to obtain the memory data of the transponder (15). The data may then be displayed to an operator on a display (41). The priority date of this patent is not proper for use in 35 USC 102 or 103 rejections.

- FREDERICK W RICHARD et al., (US), Article-information display system using electronically controlled tags, Patent Number: US5537126 , Publication date: 1996-07-16; IPC Classification: G06F17/60. This invention is about a product information display system has electronic display tags for displaying pricing and product information for products in stores or warehouses. The electronic display tags are electromagnetically coupled to a conductor. A control circuit is used to generate an information signal which contains a tag address and related data. A modulator circuit modulates an a-c. power signal with the information

signal and applies it to the conductor for transmission to the display tags. Each of the display tags is equipped with a coil that is electromagnetically coupled to the conductor for picking up the signals carried by the conductor. A demodulator is used to demodulate the signal picked up by the coil to obtain the original information signal. Each of the display tags is provided with a manually operated switch for initializing the tags with initial addresses transmitted by the conductor. A microprocessor in the electronic tag then compares the address contained in subsequent information signals with the address stored in the tag's memory. If the addresses match, the microprocessor further processes the information signal for visual display or verification functions. This invention doesn't show that tags containing routing information of the attached manufactured product.

- WANG FENGYUAN (CN), Commercial goods certificate anti-counterfeit detecting system adaptive for network station query, Patent Number: CN1346102

Publication date: 2002-04-24; IPC Classification: G06F17/30.

This patent is directed to a commodity certificate antifalse detection system applicable to web station inquiry, mainly including a special-purpose inquiry web station, said special inquiry web station possesses the data base formed from product or certificate antifalse codes inputted by

manufacturer or certificate-issuing mechanism, and the antifalse code on the product or certificate is formed from digital bar code, English serial number code and English cipher code. Said invention utilizes the timelines and interaction property of network so as to make antifalse inquiry process simple and quickly and can raise antifalse accuracy.

- CHEN MINGFA (CN) , STRUCTURE VEIN ANTI-COUNTERFEIT METHOD;
Patent Number: EP1193668, Publication date: 2002-04-03, IPC
Classification: G09F3/00. This invention is directed to a method for discerning false from genuine. The method increases the difficulty of imitation by means of using the intrinsic stochastic structural vein of the material itself as identification. According to the method, it is advisable to select the material with clear stochastic structural vein as marker, and to select the stochastic structural vein of the marker as identification information, the information is recorded by scanner and then is stored into the database of the computer identification system. Consumers may obtain relevant information of structural vein by telephone, fax or computer on line to testify whether a product is genuine or a counterfeit.

- TIAN YU (CN) , THREE DIMENSION ANTI-COUNTERFEIT METHOD,
Patent Number: WO0223512, Publication date: 2002-03-21,
IPC Classification: G09F3/00 .This invention provides a

three dimension anti-counterfeit method which relies on the financial-net, telecommunication-net and internet and uses a three dimension anti-counterfeit card as an identifier. Two groups of numerals which are attached to the anti-counterfeit card are encrypted and produced by a computer. One group of numeral is clear and the other group of numeral is unclear. Every product is provided with a sole anti-counterfeit card, while two groups of numerals which are attached to the anti-counterfeit card are stored in an anti-counterfeit information database which is connected with the financial-net, telecommunication-net and internet, thereby one-to-one correspondence relationship is formed. When a consumer wants to know the truth and falsehood of product, he can select the relevant network and its inquiry tool and carry on the inquiry. Then he can distinguish the truth and falsehood of product by magnetic card, IC card, telephone and internet.

- OUTWATER CHRIS, PRODUCT AUTHENTICATION SYSTEM AND METHOD

Patent Number: WO0062238, Publication date: 2000-10-19, IPC Classification: G06K7/10. This invention is directed to a product (20) authentication system and method employs a unique mark (10) that is simple and cost-effective to apply,

but provides several layers of protection, including anti-counterfeit and anti-diversion, against counterfeits. The unique mark (10) contains a product control code that is printed in invisible ink comprising a UV ink and an IR ink. The first layer of protection is invisible. The second layer of protection is the code itself. The third layer of protection is the presence of the IR ink in the invisible code. The fourth layer of protection is the IR emitting characteristics of the invisible code.

- Debbie Galante Block, Piracy of sound recordings, videos, and computer programs has increased in the 1990s in spite of the efforts of anti-piracy groups to ban the practice. From Emedia Professional, December 01 1998, 9 pages.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CUONG H. NGUYEN whose telephone number is 703-305-4553. The examiner can normally be reached on 7am - 3:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas G. Black can be reached on 703-305-8233. The fax phone number for the organization where this application is assigned is 703-305-7687.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Cuonghnguyen

CUONG H. NGUYEN
Primary Examiner
Art Unit 3661